D34: Méthodes de calcul efficaces
TD n 1: arithmétique multiprécision

1 Exercices

Exercice 1. Algorithmes multiprécision

1. Faire la somme et le produit des entiers suivants en base 16: $a = 56FA2$ et $b = 35CD1$.
2. Calculer le quotient et le reste de la division euclidienne des polynomes $2X^4 + 7X^3 + X + 2$, $X^5 - 1$ et $X^4 + X^3 + X^2 + X + 1$ par $X^2 + X + 1$.

Exercice 2. Algorithme de Karatsuba

1. Appliquer, de façon détaillée, l'algorithme de Karatsuba pour calculer le produit des polynômes $X^3 + 2X^2 - 3X + 1$ et $4X^3 + X^2 - X - 1$.
2. On considère des polynomes de degré 2:$A[X] = A_2X^2 + A_1X + A_0$ et $B[X] = B_2X^2 + B_1X + B_0$:
   1. Calculer les coefficients $C_0, \ldots, C_4$ du produit $C[X] = A[X]B[X]$. Combien de multiplication sont nécessaires?
   2. En utilisant une approche similaire à celle de Karatsuba, montrer qu'il est possible d'effectuer ce calcul en seulement 6 multiplications.
   3. En déduire un algorithme de multiplication des polynomes de degré $3^t - 1$. Quelle est sa compléxité?

Exercice 3. Algorithme de Toom-Cook

1. Appliquer, de façon détaillée, l'algorithme Toom-3 pour calculer le produit des polynomes $X^2 + 3X + 2$ et $2X^2 - 3X + 1$.
2.
   1. Décrire l'algorithme de Toom-Cook dans le cas $k = 2$ (découpage en 2). En quels points peut-on évaluer les polynomes pour simplifier les calculs?
   2. Donner les formules permettant de calculer les valeurs du polynôme produit en ces points.
   3. En déduire la matrice d'interpolation TC2 permettant d'obtenir les coefficients du polynôme produit.
   4. Quelle est la compléxité de cette méthode?

2 Programmation

Exercice 1. Seuils d'efficacité

Le but de cet exercice de réaliser une implantation de différents algorithmes de multiplications afin dans comparer les performances. L'étude devra notament mettre en évidence les différents seuils d'éfficacité des algorithmes. Pour cela, vous utiliserez le type `bignum` dont les fonctions élementaires sont fournies dans le fichier `bignum.c`. Le ficher header correspondant contient les informations nécessaires pour manipuler les grands nombres.

1. Écrire le fichier `bn_arith.c` correspondant au fichier d'entete `bn_arith.h`. Le but est d'implanter l'algorithme de multiplication multi-précision des livres d'écoles. Pensez à uiliser la bibliothéque `gmp` pour vérifier la validité de votre implantatio n.
2. Implanter l'algorihtme de Karatsuba puis . Effectuer une expérience numérique afin de mettre en évidence le seuil d'efficacité de chaque algorithme.